LATERAL NEWS — LATERALCODE

Perché iceGate e la tecnologia ZeroSurface® proteggono (davvero) dal phishing?

2 maggio 2023

(…anche se clicchi come un disperato su ogni link che ti propongono!)

Ce lo dicono in tutte le salse: nella sicurezza informatica l'anello più debole della catena è sempre l'uomo con il suo comportamento. Benché semplicistica, l'affermazione ha un suo senso (ma ne parleremo meglio in un'altra occasione) e il **phishing** è lì a dimostrarlo: inseriamo i nostri dati in siti e ambienti **fake** e non c'è 2FA che tenga se la trappola è ben costruita e se il target è di quelli importanti o di quelli che giustificano un APT, cioè un team e risorse dedicate.

Una volta infranto e oltrepassato **il primo livello di attenzione** (quello che ci metterebbe in allarme se solo leggessimo e osservassimo più attentamente mail, link, siti o URL vari) la strada è in discesa, un masso che, rotolando, porta con sé le nostre credenziali: ci ritroviamo su pagine "note", colori, immagini e form **familiari** e… l'abitudine fa il resto.

I dilettanti hackerano i sistemi, i professionisti hackerano le persone — (Bruce Schneier)

LA FONDAMENTALE DIFFERENZA

Certo, anche una soluzione come **iceGate**, che è il sistema di sicurezza perimetrale **ZeroSurface®** di LATERALCODE, ha bisogno di un passaggio in cui accertarsi che **voi-siete-voi**, ma lo fa con **cruciali differenze**.

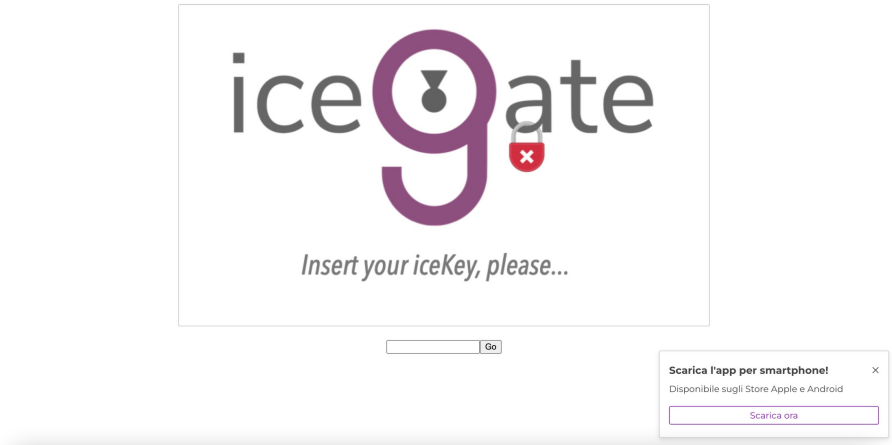
Con **ZeroSurface®** infatti il **punto di autenticazione**:

1. non è mai “bordo rete”
2. non è riconducibile né fisicamente né logicamente al sito **target**
3. risponde a un URL che è esso stesso uno fattore di autenticazione (dettaglio fondamentale, come sarà chiaro tra poco)

IL NECESSARIO SPIEGONE (ma prima la breve necessaria premessa sull’uso di una soluzione ZeroSurface®…)

Come forse sapete, una protezione **ZeroSurface®** rende **irraggiungibile(!)** il vostro target, **scansioni comprese**: di fatto **spegne la presenza in rete** delle vostre applicazioni pubbliche (non a caso la risposta che riceviamo dai **portscan** è roba tipo “host seems down” e simili). Voi e/o i vostri clienti dovete però poter usare i vostri servizi e quindi dovete autenticarvi (nel caso mostrato qui tramite una semplice pagina web, ma via app mobile il principio è lo stesso).

Bene, questo è lo screenshot di una pagina di autenticazione di **iceGate**.



La pagina di autenticazione di iceGate: ogni cliente ha la propria, anonima e non parlante, ma tutte hanno la stessa identica grafica.

Questa pagina è graficamente uguale per tutti gli utenti ma ognuno di essi può essere riconosciuto **SOLO dalla pagina a lui assegnata** che risponde a un **URL anonimo e non parlante** e, ancora una volta, mai riconducibile né fisicamente né logicamente al sito target; qualcosa del tipo *https://gretkky.org/j47Id3e* e via di fantasia.

Riassumendo, dunque, le credenziali **minime** necessarie per accedere a una rete protetta da **ZeroSurface®** sono **una URL e una password**.

Una volta inserita la password, la “iceKey”, l’utente riceve questo messaggio:

Se la iceKey è corretta, il sistema restituisce un generico “ACCESS GRANTED”, ma SOLO l’utente legittimo SA per quale servizio o applicazione è stato autorizzato: la pagina NON effettua redirect.

…e non succede altro!

Niente refresh, niente **redirect** e, no, niente token di vario tipo trasmessi al browser (fondamentale)!

Ora, **per lui SOLO e per nessun altro in rete**, il punto d’accesso al suo servizio diviene visibile. Non dovrà fare altro che aprire la sua applicazione, il suo servizio, il suo sito ecc., accedere e lavorarci comodamente, sapendo che per il resto del mondo **rimarrà tutto assolutamente irraggiungibile**.

Bene, fine dello spiegone.

LA FELICE CONSEGUENZA

Ora pensate a come funziona il **phishing**:

- noi consegnamo “volontariamente” le credenziali ad ambienti che ci paiono familiari, abituali
- in maniera asincrona (più spesso) o in maniera sincrona (meno spesso e per i casi a maggior budget disponibile per gli attaccanti) quelle credenziali vengono sottratte e usate da terzi malintenzionati
- a questo punto il criminale “è noi” e può fare quel che vuole

Ed eccoci al punto.

Immaginate che il cattivo sia riuscito a “pescare” **user** e **password** relativi al vostro solito servizio, che abbia violato il 2FA (accade più spesso di quanto vorremmo ammettere!) e che addirittura **vi abbia sottratto la iceKey** magari perché ha riprodotto una pagina identica a quella vista poco fa, su cui vi ha indirizzato (non si sa come e non ci interessa tanto ZeroSurface® funziona lo stesso): e allora?

Non potrebbe entrare lo stesso e il motivo è evidente (lo è?)!

Vediamo. Nel **phishing** viene ricreato un ambiente familiare grazie al quale vi sentite tranquilli nell’usare le vostre credenziali (che invece vi vengono sottratte). Nel caso di **iceGate**, però, non basta ricreare graficamente la pagina di autenticazione (per altro di una essenzialità disarmante) bensì è necessario che quella pagina sia quella **ORIGINALE** (cioè quella funzionale!), cosa che nel **phishing** (e non solo) ovviamente non può essere riprodotto; in altre parole, l’attaccante non può farvi autenticare **sull’unico vero URL in grado di accogliere UTILMENTE l’iceKey** (né potrà farlo lui perché non può conoscerlo).

Pensateci: per un utente di **iceGate** (e per chiunque di noi, in fondo) l'ambiente "familiare" in cui inserire un URL è la barra degli indirizzi del suo browser, **non la form di un sito!** E poi, quel **fattore fondamentale**, l'URL funzionale, come potrebbe essere mai "pescato"?

Insomma, se voi perdete le chiavi di casa vostra durante un viaggio a Tokyo e se quelle chiavi non hanno un portachiavi che ne suggerisca la provenienza (se cioè sono "anonime e non parlanti"), al ritorno in patria vi preoccupate di cambiare la serratura?

Ecco, con **ZeroSurface®** è la stessa cosa: possono "pescare" tutte le vostre chiavi ma **non sapranno mai quale e dove sia la serratura…**

Premiati da oltre 200 CIO…

Lateral News — Articoli, idee e riflessioni sullo sviluppo tecnologico e sulla sicurezza informatica non "mainstream"

lateralcode.it